

**Technical Support Services  
for the Medicaid  
HIPAA-Compliant  
Concept Model  
(MHCCM)**

**HIPAA Privacy Risk Assessment Checklist  
(For Medicaid State Agency Self-Assessment)**

**April 19, 2002**

**Prepared for:  
Centers for Medicare & Medicaid Services  
Center for Medicaid and State Operations  
7500 Security Boulevard  
Baltimore, MD 21244 – 1850**

# HIPAA PRIVACY PROJECT ASSESSMENT CHECKLIST (STATE SELF-ASSESSMENT)

This risk assessment checklist is provided as a self-assessment tool to allow States or agencies to gauge where they are in the overall picture of HIPAA Privacy implementation. This checklist is intended to be used by the HIPAA Privacy Coordinator/Project Lead, or other key agency representative in the State, Medicaid agency, or other agency. Use of this checklist is voluntary; it is intended to assist the agency and is not required to be submitted to CMS.

The Yes column following each item can be checked if the person completing it can respond positively to the question (i.e., the item is completed or in progress). The Yes column can also be checked if adequate resources and planning have been allocated for future efforts. If these criteria are not met, the No column should be checked. Two critical parameters often appear in the question sets. The first addresses whether a thorough analysis was performed resulting in a clear understanding of the task in question. The second addresses whether a firm commitment of specific allocation of funds and/or resources exists to accomplish the task.

There are no official score sheets or right or wrong answers; the list of questions is provided as an aid to help establish a barometer of progress and highlight work still needing to be accomplished. The list is also intended to provide ideas on areas that States or agencies may not have considered in their project efforts toward HIPAA compliance. It is in the organization's best interest to answer the questions as honestly and accurately as possible. The HIPAA Privacy Coordinator/Project Lead is usually in the best position to provide accurate answers to the questions and can act as the best judge of the status of each project area in the checklist.

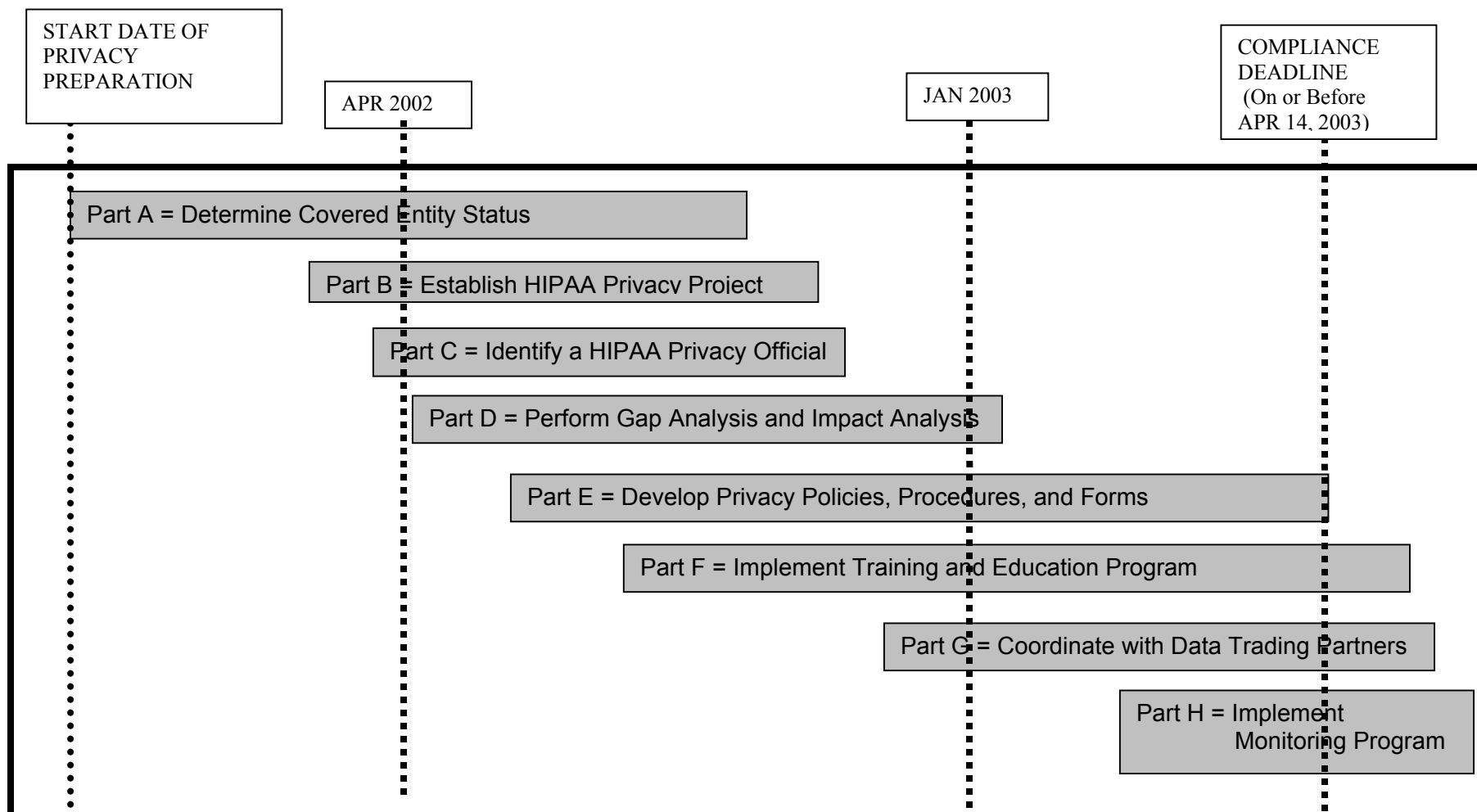
**Each question for which a No answer was supplied should be examined, and the reason for which No was given should be understood. If, in fact the No answer is proper for the activities required to become HIPAA compliant, it need not be considered further and N/A can be put in the answer boxes. The checklist is intended to serve as a tool for identifying areas of risk. Every No answer remaining after the analysis is an indication of an area of risk. The more remaining Nos, the higher the risk for achieving Privacy compliance. In general, the project is at low risk if the answers are mainly Yes or N/A. However, even in the case of many No responses to the questions, this checklist is not intended to give the impression that the organization is not going to successfully achieve HIPAA compliance. It should allow better focus of organization efforts in the time remaining until April 14, 2003.**

Please be aware that this checklist only applies to the Privacy Rule (Rule 2). Rule 1, Transactions, must also be implemented in this time period. Activities pertaining to Rule 1 are not included in this checklist. There is a separate checklist available for Rule 1.

The timeline graphic illustrates the overlapping of project phases and activities and the overall chronology of project activity. The timeline also provides comparison dates of April 2002, and January 2003, to provide a general indication of where each organization should be in the project timeline. This is a depiction of an "ideal project". Roughly, a Privacy Project can correlate its own timeline to this one by aligning its actual start date with this timeline's start date and then comparing its tasks and activities with the timeline for the 8 defined project areas (A-H).

Sources for useful HIPAA-related information are suggested in some of the checklist items below (CMS white papers can be found at either [WWW.MHCCM.ORG](http://WWW.MHCCM.ORG) or [WWW.CMS.GOV](http://WWW.CMS.GOV)).

## PLOTTING THE PROJECT TIMELINE



# HIPAA PRIVACY RISK ASSESSMENT CHECKLIST – State Self-Assessment

## Checklist Contents

- Part A – Determine Covered Entity Status
- Part B – Establish HIPAA Privacy Project
- Part C – Identify a HIPAA Privacy Official
- Part D – Perform Gap Analysis and Impact Analysis
- Part E – Develop Privacy Policies, Procedures, and Forms
- Part F – Implement Training and Education Program
- Part G – Coordinate with Data Trading Partners
- Part H – Implement Monitoring Program

## **Part A – Determine Covered Entity Status**

### **1. Determine Covered Entity Status**

*Determining Medicaid covered entity status is the first step on the road to HIPAA Privacy compliance.*

	Yes	No
Has the Medicaid Agency reviewed each program it administers based upon the Privacy Regulation?		
Has the Medicaid Agency defined its covered entity status based on the Privacy Regulation?		

## **Part B – Establish HIPAA Privacy Project**

### **2. Establish a HIPAA Project Office**

*The HIPAA Privacy Project Office can be statewide, agency-wide, or department specific.*

	Yes	No
Is a HIPAA Privacy Project Office established?		
Does the HIPAA Privacy Project Office have support at the highest State executive levels?		
Is there a current organization chart and charter document?		
Is the Privacy Project Lead required to periodically report the project status to senior management?		
Are HIPAA Privacy Project Office responsibilities, and tasks (scheduling, tracking and reporting functions) consistent with their structure in the state organization?		

### **3. HIPAA Privacy Budgets, Resources, and Contracts**

*Resources must be identified and available to complete identified tasks in the work plan.*

	Yes	No
Is there a budget for HIPAA Privacy compliance?		
Is there a resource plan?		
Are the staffing requirements assessed for the entire project?		
Are staffing resources available when needed?		
Does the HIPAA Privacy Project Office have a firm commitment of resources and staff to meet the requirements?		
Are any needed services and support contracts in place?		

### **4. State or Agency HIPAA Privacy Project Work Plan**

*Overall State plan should include State agency coordination. May need sub-plans and questionnaire for specific areas, associated offices or subordinate departments.*

	Yes	No
Is there an overall State or Agency (or comparable) HIPAA Privacy Project Work Plan?		
If needed, are there individual department Privacy work plans?		
Are reasonable timelines established for critical activities?		
Are specific individuals responsible for updating the plan?		
Does the plan include outreach activities to other State agencies and business associates?		
Has the latest Privacy NPRM been analyzed to determine its impact on the Agency's Privacy Plan?		

## 5. Security Implications

*Even though the Security Standard has not been issued, adequate security to protect health information is required to assure privacy.*

	Yes	No
Has the Agency identified security requirements needed for Privacy compliance?		
Has the Agency assessed its security processes?		
Is there a plan to enhance security procedures to support Privacy requirements?		

## 6. Scheduling and Tracking Project Activities

*Individual plans & schedules for the Privacy implementation effort must be tracked.*

	Yes	No
Do HIPAA schedules define tasks and milestones, indicating responsible entities and dependencies?		
Are there processes and tools to support maintaining HIPAA project plans and schedules?		
Is a process for identifying, reporting, tracking, and monitoring all issues to resolution in place?		
Does this process include a mechanism for resolution of interagency issues?		
Do all departments, divisions, and units report their progress and status to the Privacy Project Office?		
Is there periodic executive level review of progress and deadlines?		

## **Part C – Identify a HIPAA Privacy Official**

### **7. Define the Privacy Official Role**

*The Privacy Official has a role defined in the federal law. The job description needs to be consistent with this level of responsibility.*

	Yes	No
Has the State Agency documented the responsibilities of the Privacy Official?		
Has legal counsel ruled on the adequacy of the documented role?		
Is the HIPAA Privacy Official position at a level consistent with the range of responsibilities associated with the Covered Entity, e.g., if the covered entity is the Agency, does the Privacy Official report directly to the Secretary or Director of the Agency?		
Does the Privacy Official have authority to impose Privacy policies and procedures throughout the Medicaid enterprise?		
Does the Privacy Official have adequate authority to carry out the directives of the role?		

### **8. Designate a HIPAA Privacy Official**

*The HIPAA Privacy Official needs to have an appropriate level of authority within the covered entity.*

	Yes	No
Has the State named a HIPAA Privacy Official?		
Does the Privacy Official have dedicated staff (salaried or contractor)?		

## **Part D – Perform Gap Analysis and Measure Impact on Medicaid Facilities, Systems, and Business Processes**

### **9. Perform Gap Analysis**

*If the State statutes are demonstrated to be more restrictive than the federal regulation, the State laws will take precedence. Burden of proof is on the State.*

	Yes	No
Has the State compared the HIPAA Privacy regulation with all relevant State privacy and confidentiality statutes?		
Has the State determined whether or not the State statutes are more restrictive than the federal?		
Has there been a legal opinion given on the status of State statutes?		
Has the total set of privacy requirements (Federal, State, Agency) been documented?		
Does the Agency have a Privacy questionnaire to assess the Privacy gaps throughout the Agency?		
Does the questionnaire cover all requirements of the Privacy Regulation?		
Has the questionnaire been widely distributed to all levels of staff in all divisions and units/locations?		
Will responses be captured for analysis?		
Has the Agency documented and analyzed the gaps between requirements and current Privacy status?		
Will the questionnaire results be correlated with the respondent's staff position?		
Has the Agency updated the gap analysis based on survey results?		

### **10. Business Processes: Inventory, Impact, and Re-Engineering**

*Business Processes must be assessed for HIPAA Privacy impact, and prioritized for re-engineering (requiring changes in policy, procedure, training and use of data).*

	Yes	No
Have Medicaid business processes and functions been inventoried?		
Has the inventory been verified against the business functions identified in the MHCCM Operations Perspective?		
Have the business processes been assessed for Privacy impact?		
Have the changes needed been developed and documented?		
Can all impacted business processes be ready by the Privacy compliance date?		
Are all facility or locations identified?		
Are building or space modifications required?		
Have all agency information systems and communications networks that store, maintain, or transmit		

PHI been identified?		
Can the Agency's information system implement the security and process requirements needed for Privacy compliance?		

## **Part E – Develop Privacy Policies, Procedures, and Forms**

### **11. Identify Policies, Procedures, and Forms that Need to Be Developed for Privacy**

*Developing and deploying Privacy policies and procedures is at the heart of meeting compliance requirements. It can be a significant, labor-intensive undertaking.*

	Yes	No
Does the Agency have a standard process to manage/oversee development of policies and procedures for Privacy?		
Does the Agency have existing confidentiality policies and procedures?		
Have current policies and procedures been compared to HIPAA Privacy requirements?		
Has the Agency developed an information practices statement, consent forms and authorization forms?		
Has the Agency developed policy and procedure templates in accordance with HIPAA standards?		
Has the Agency developed a list of all procedures required by the HIPAA Privacy Rule?		
Has the Agency compared its program policies and procedures for the release and disclosure of information to HIPAA privacy standards, including: 164.530(a) Standard: Personnel Designations 164.502(b) Minimum Use and Disclosure of PHI 164.530(b) Standard: Training 164.530(c) Standard: Safeguards 164.530(d) Standard: Complaints to the Covered Entity 164.530(e) Standard: Sanctions 164.530(f) Standard: Mitigation 164.530(g) Standard: Refraining from Intimidating or Retaliatory Acts 164.530(h) Standard: Waiver of Rights 164.530(i) Standard: Policies and Procedures 164.530(j) Documentation		
Has the Agency drafted changes to existing policies and procedure for each standard as required by HIPAA?		
Does the Agency know how many <u>new</u> policies and procedures are needed to ensure all HIPAA requirements are met?		

Is there an approval process for policies and procedures?		
Is there a plan to update policies and procedures with regulatory changes or at periodic intervals, e.g., after the latest Privacy NPRM is final?		

## **Part F – Implement Training and Education Program**

### **12. Develop and Implement Staff Training and Education Program(s)**

*For Privacy to be successfully implemented, all staff must be trained in the policies and procedures.*

	Yes	No
Does the Agency know how many staff need to be trained in Privacy policy and procedures?		
Does the Agency have a training plan to reach all employees?		
Does the training program include a course curriculum, training materials, and periodic updates?		
Is the training program structured to target specific business functions and specific staff job descriptions?		
Has the training program been tested?		
Has the training program been implemented?		
Has the training program been reviewed by legal counsel?		

## **Part G – Coordinate with Data Trading Partners**

### **13. Outreach to Business Partners**

*Inclusion of the State Medicaid Enterprise. For guidance, see the CMS paper “OUTREACH TO DATA TRADING PARTNERS: “You’re OK, I’m OK”.*

	Yes	No
Does the agency have a Privacy Outreach Plan?		
Has the agency identified all business associates and trading partners to be included in the outreach efforts?		
Has a survey been sent to providers to determine their HIPAA Privacy compliance status?		
Are providers able to send and receive encrypted data?		

## 14. Agreements

*Trading Partner agreements need to be updated for Privacy.*

	Yes	No
Has language regarding mutual Privacy provisions been evaluated for addition to Trading Partner agreements?		
Has the Agency identified all Trading Partners whose agreements should contain privacy provisions?		
Was legal counsel involved in developing the contract language and changes?		
Has the State determined what protected health information is provided to which partners, and that the PHI is appropriate for the business purposes?		
Does the State have a process for developing contract amendments as necessary to meet HIPAA requirements to safeguard protected healthcare information?		
Are contracts filed in a secure place?		
Have all business associate contracts been examined in light of the Privacy Regulation?		
Are all needed parts of these contracts rewritten to ensure HIPAA Privacy compliance?		

## **Part H – Implement Monitoring Program**

### 15. Develop and Implement a Monitoring and Oversight Program

*The Agency is required to oversee and monitor its Departments to determine Privacy compliance.*

	Yes	No
Does the agency have designated resources for ongoing oversight, maintenance, and resolution of issues and complaints (e.g. Privacy official and other staff)?		
Does the Agency have an auditing function to determine staff compliance with HIPAA privacy requirements?		
Has this function been staffed and are auditors trained?		
Does the audit function have a budget?		
Has the audit program been reviewed by legal counsel?		